EXHIBIT 14

UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone

GENEVA (22 January 2020) - UN human rights experts are gravely concerned by information they have received suggesting that, in contravention of fundamental international human rights standards, a WhatsApp account belonging to the Crown Prince of the Kingdom of Saudi Arabia in 2018 deployed digital spyware enabling surveillance of *The Washington Post* owner and Amazon CEO, Jeffery Bezos.

The independent experts – Agnes Callamard, UN Special Rapporteur on summary executions and extrajudicial killings, and David Kaye, UN Special Rapporteur on freedom of expression – said the following:

"The information we have received suggests the possible involvement of the Crown Prince in surveillance of Mr. Bezos, in an effort to influence, if not silence, The Washington Post's reporting on Saudi Arabia. The allegations reinforce other reporting pointing to a pattern of targeted surveillance of perceived opponents and those of broader strategic importance to the Saudi authorities, including nationals and non-nationals. These allegations are relevant as well to ongoing evaluation of claims about the Crown Prince's involvement in the 2018 murder of Saudi and Washington Post journalist, Jamal Khashoggi.

"The alleged hacking of Mr. Bezos's phone, and those of others, demands immediate investigation by US and other relevant authorities, including investigation of the continuous, multi-year, direct and personal involvement of the Crown Prince in efforts to target perceived opponents.

"This reported surveillance of Mr. Bezos, allegedly through software developed and marketed by a private company and transferred to a government without judicial control of its use, is, if true, a concrete example of the harms that result from the unconstrained marketing, sale and use of spyware. Surveillance through digital means must be subjected to the most rigorous control, including by judicial authorities and national and international export control regimes, to protect against the ease of its abuse. It underscores the pressing need for a moratorium on the global sale and transfer of private surveillance technology.

"The circumstances and timing of the hacking and surveillance of Bezos also strengthen support for further investigation by US and other relevant authorities of the allegations that the Crown Prince ordered, incited, or, at a minimum, was aware of planning for but failed to stop the mission that fatally targeted Mr. Khashoggi in Istanbul.

At a time when Saudi Arabia was supposedly investigating the killing of Mr. Khashoggi, and prosecuting those it deemed responsible, it was clandestinely waging a massive online campaign against Mr. Bezos

and Amazon targeting him principally as the owner of The Washington Post."

The two experts – who were appointed by the Human Rights Council - recently became aware of a 2019 forensic analysis of Mr. Bezos' iPhone that assessed with "medium to high confidence" that his phone was infiltrated on 1 May 2018 via an MP4 video file sent from a WhatsApp account utilized personally by Mohammed bin Salman, the Crown Prince of the Kingdom of Saudi Arabia. According to the analysis, the Crown Prince and Mr. Bezos exchanged phone/WhatsApp numbers the month before the alleged hack. The forensic analysis found that within hours of receipt of the MP4 video file from the Crown Prince's account, massive and (for Bezos' phone) unprecedented exfiltration of data from the phone began, increasing data egress suddenly by 29,156 per cent to 126 MB. Data spiking then continued undetected over some months and at rates as much as 106,032,045 per cent (4.6 GB) higher than the pre-video data egress baseline for Mr. Bezos' phone of 430KB.

The forensic analysis assessed that the intrusion likely was undertaken through the use of a prominent spyware product identified in other Saudi surveillance cases, such as the NSO Group's Pegasus-3 malware, a product widely reported to have been purchased and deployed by Saudi officials. This would be consistent with other information. For instance, the use of WhatsApp as a platform to enable installation of Pegasus onto devices has been well-documented and is the subject of a lawsuit by Facebook/WhatsApp against NSO Group.

The allegations are also reinforced by other evidence of Saudi targeting of dissidents and perceived opponents. For instance, the United States has brought criminal proceedings against two Twitter employees and a Saudi national "for their respective roles in accessing private information in the accounts of certain Twitter users and providing that information to officials of the Kingdom of Saudi Arabia". All three individuals are charged with being illegal agents for Saudi Arabia who, according to U.S. prosecutors, engaged in the "targeting and obtaining private data from dissidents and known critics, under the direction and control of the government of Saudi Arabia".

The Special Rapporteurs note that the allegations regarding the hacking of Bezos' mobile phone are also consistent with the widely reported role of the Crown Prince in leading a campaign against dissidents and political opponents. The hacking of Mr. Bezos' phone occurred during a period, May-June 2018, in which the phones of three close associates of Jamal Khashoggi, Yahya Assiri, Omar Abdulaziz and Ghanem Al Masarir were also hacked, allegedly using the Pegasus malware.

At the time of the alleged May 2018 hack of Mr. Bezos' phone, Jamal Khashoggi was a prominent columnist for *The Washington Post* whose writing increasingly raised concerns about the Crown Prince's rule. On 2 October 2018, Saudi government officials murdered Mr. Khashoggi in the Saudi consulate in Istanbul, Turkey. *The Post* quickly began its substantial coverage of the disappearance and murder investigation, expanding into reporting a number of related aspects of the Crown Prince's rule in Saudi Arabia.

According to the forensic analysis, following the hacking of Mr. Bezos' phone, the Crown Prince sent WhatsApp messages to Mr. Bezos, in November 2018 and February 2019, in which he allegedly revealed private and confidential information about Mr. Bezos' personal life that was not available from public sources. During the same period, Mr. Bezos was widely targeted in Saudi social media as an alleged adversary of the Kingdom. This was part of a massive, clandestine online campaign against Mr. Bezos and Amazon, apparently targeting him principally as the owner of *The Washington Post.* The UN experts further note that Mr. Saud al-Qahtani, named by the Saudi prosecutor as having incited the kidnapping of Mr. Khashoggi, was also linked repeatedly to the organization of the on-line campaign excoriating *The Post* and calling for boycotts of Mr. Bezos and his companies.

The annexes to this statement provide detail concerning the expert forensic analysis of Mr. Bezos' device that took place in 2019.

The Special Rapporteurs expect to continue their investigations into responsibility for the murder of Mr. Khashoggi and the growing role of the surveillance industry in permitting the unaccountable use of spyware to intimidate journalists, human rights defenders, and owners of media outlets.

ENDS

Annex I and II

Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi

2019 report on the private surveillance industry to the United Nations Human Rights Council is now available online

*Ms. **Agnes Callamard**, UN Special Rapporteur on summary executions and extrajudicial killings, investigated and reported to the Human Rights Council in 2019 evidence showing the role of the Government of Saudi Arabia in the murder of journalist Jamal Khashoggi.*

*Mr. **David Kaye**, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, reported to the Council at the same time on the growing and lawless use of malicious spyware to surveil and intimidate journalists, human rights defenders, and others in civil society.*

The Special Rapporteurs are part of what is known as the Special Procedures of the Human Rights Council. Special Procedures, the largest body of independent experts in the UN Human Rights system, is the general name of the independent fact-finding and monitoring mechanisms of the Human Rights Council that address either specific country situations or thematic issues in all parts of the world. Special Procedures experts work on a voluntary basis; they are not UN staff and do not receive a salary for their work. They are independent from any government or organisation and serve in their individual capacity.

UN Human Rights country page – Saudi Arabia

***For inquiries and media requests**, please contact: Mr. Bach Avezdjanov (+1 212 854 6785) or write to ba2482@columbia.edu*

*For **media inquiries** related to other UN independent experts please contact:*

*Mr. Jeremy Laurence (+41 22 917 9383 **/** jlaurence@ohchr.org)*

Follow news related to the UN's independent human rights experts on Twitter @UN_SPExperts.

Concerned about the world we live in?

Then STAND UP for someone's rights today.

#Standup4humanrights and visit the web page at http://www.standup4humanrights.org